УДК 004.771

О. В. Рябцева
Научный руководитель: А. Е. Баринов
Южно-Уральский государственный университет, Челябинск

КРИТЕРИИ НАЧАЛА ПРОВЕДЕНИЯ ПОВТОРНОГО АНАЛИЗА РИСКОВ ИБ В АСУ ТП

Аннотация. Описано понятие АСУ ТП. Анализируются проблемы выбора способов обеспечения безопасности. Рассмотрена проблема выбора критериев своевременного повторного анализа исков ИБ в АСУ ТП. Проведен обзор процесса оценки рисков и методологии их определения. Цель исследования заключалась в анализе рисков безопасности автоматизированных систем управления технологическими процессами. Определены потребности в анализе ИБ, задачи управления рисками. Рассмотрен план проведения анализа. Авторами определены основные угрозы безопасности в автоматизированных системах управления технологическими процессами.

Ключевые слова: информационная безопасность; защита информации; автоматизированная система управления технологическими процессами; анализ ИБ; оценка риска.

Для любого предприятия, обладающего сложными технологическими процессами, задачи повышения эффективности производства и обеспечения нового качества управляемости являются многозначащими. Автоматизированная система управления технологическими процессами (АСУ ТП) представляет собой инструмент для решения данных задач. Она состоит из группы персонала, совокупности аппаратного и программного обеспечений.

В процессе управления необходимо вырабатывать осознанные и эффективные решения, которые можно принять только на основании фактов и анализа причинно-следственных связей [1]. В обеспечение безопасности АСУ ТП необходимо уделять внимание не только обеспечению конфиденциальности, а также обеспечению непрерывности и целостности данных технологического процесса. Безопасность технологического процесса — это прежде всего безопасность жизни и здоровья людей [1]. Поэтому большую роль приобретает анализ рисков ИБ в АСУ ТП.

Анализ информационной безопасности является начальным и основным этапом в процессе построения и внедрения системы защиты информации. **Оценка риска** — это процесс, при котором в количественном или качествен-

ном выражении определяется величина ущерба или убытка [1]. На сегодняшний день существуют несколько методологий определения оценки рисков:

- анализ и управление рисками — CRAMM;
- управление рисками в системе информационных технологий — NIST SP800-30;
- оценка активов и уязвимости информационной безопасности — OCTAVE;
- информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности — ISO/IEC 27005:2011.

Необходимо отметить, что табл. 1 основана на выбранном числе значения атрибутов соответствующих шаблонов, используемых для описания методов. Эти атрибуты считаются наиболее подходящими для краткого сравнения [2].

Таблица 1

Сравнение методов определения рисков

Атрибуты / Методы	Определение риска	Анализ риска	Оценка риска	Обмен рисками	Необходимые навыки
CRAMM	•••	•••	•••		***
NIST SP800-30	•••	•••			**
OCTAVE	••	••	••	••	**
ISO 27005	••	••	••	•••	**

Уровень навыка: * — базовый уровень, ** — стандартный уровень, *** — специализированный уровень. Количество отметок (•, ••, •••), используемых в этих атрибутах, варьируется от 3 до 3. Они определяют степень выполнения фазы рассмотренными методами.

К основным угрозам безопасности АСУ ТП можно отнести:

- внешнее проникновение с выведением АСУ ТП и управляемых объектов из строя;
- внешнее несанкционированное управление технологическими объектами с определенными целями;
- несанкционированное внесение изменений в ПО для изменения режимов работы технологических объектов.

При помощи руководства и сотрудников необходимо определить область угроз ИБ. После чего возникает деятельность, состоящая в определении направления целевого состояния обеспечения ИБ. Согласно ГОСТ 62443-2-1–2015 в ходе внедрения системы управления кибербезопасностью АСУ ТП требуется определить плановую периодичность и критерии повторного анализа рисков. Стандарт [3] определяет примерный набор критериев, однако он явно не является исчерпывающим. В частности отметим критерии, не обозначенные в нем, но имеющие весомое значение:

– слияние компаний, открытие новых офисов или филиалов;
– смене стратегии, модели управления или организационной структуры компании;
– изменения в законодательстве, связанные с ИБ;
– внедрение новых технологий, бизнес-процессов и стандартов в компании.

При слиянии компаний происходит расширения штата сотрудников, увеличение производственных мощностей и, как следствие, рост рисков ИБ. В данном случае для исключения опасности без повторного анализа не обойтись.

Смена стратегии и модели управления влечет за собой неизбежность перестройки основных компонентов АСУ ТП, в которых заложены основные факторы производства. Изменения в них являются побудителям к проведению повторного анализа рисков ИБ.

Введение штрафа за последствия от нарушения критического технологического процесса [4] подтверждает необходимость анализа рисков ИБ при изменениях в законодательстве, а также пересмотре отношения к процессу повторного анализа.

При анализе рисков понятие ситуации выражается в инвентаризации и оценке активов АСУ ТП. Без инвентаризации активов невозможно ответить на вопрос, что именно нужно защищать. Очень важно понять, какая информация обрабатывается в АСУ ТП и как выполняется ее обработка [5]. Первоочередной задачей управления рисками становится определение наиболее значимых активов. После того как активы идентифицированы, необходимо определить их ценность. Она выражается величиной потерь, которые понесет АСУ ТП в случае нарушения безопасности актива.

Таким образом, проведение повторного анализа рисков ИБ в АСУ ТП позволяет сконцентрировать внимание на наиболее актуальных проблемах и предотвратить нанесение ущерба компании.

Список литературы

1. *Суханов А.* Анализ рисков в управлении информационной безопасностью [Электронный ресурс]. 2008. Режим доступа: http://iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi-bezopasnosti/analiz-riskov-v-upravlenii-informacionnoi-bezopasnostyu.

2. European Network and information Security Agency (ENISA) // Risk Management: Implementation principles and Inventories for Risk Management / Risk Assessment methods and tools. 2006. P. 63.

3. ГОСТ 62443-2-1–2015. Национальный стандарт РФ сети коммуникационные промышленные. М., 158 с.

4. *Хабриева Т. А.* Закон. Обеспечение безопасности и реальной экономики. М., 2015. 48 с.

5. *Цапко Г. П.* Анализ рисков безопасности автоматизированных систем управления технологическими процессами // Интернет-журнал «Науковедение». 2016. № 5. С 1–9.

УДК 004.056.53

И. П. Соколов
Научный руководитель: канд. тех. наук, доцент В. В. Бакланов
Уральский федеральный университет, Екатеринбург

О БЕЗОПАСНОСТИ ПРОГРАММ С ОТКРЫТЫМ КОДОМ

Аннотация: обсуждаются проблемы информационной безопасности LINUX-программ с открытым кодом.

Ключевые слова: программное обеспечение с открытым кодом; операционная система LINUX; сетевой протокол.

Сегодня широкое распространение получили программные продукты и системы с открытым исходным кодом. Это объясняется тем, что они бесплатные и, по мнению многих, безопасные, поскольку используют открытый исходный код, который может проверить каждый желающий. С далеких времен яркими представителями операционных систем с открытым исходным кодом являются UNIX подобные системы, которые развивались энтузиастами, и порой о безопасности никто и не думал.

С появлением Linux ничего не изменилось, Linux целиком соблюдает концепции, заложенные в UNIX. Ядро Linux полностью свободно распространяемое, как и утилиты, входящие в ее комплект. Многие считают Linux неуязвимой системой. Однако Linux-системы, как выше упоминалось, разрабатываются энтузиастами, и они значительно проигрывают системам, которые разрабатываются специализированными организациями. Например, над разработкой ОС семейства Windows работают тысячи высококвалифицированных разработчиков, но даже в этом семействе операционных систем периодически находят уязвимости. Кроме того, в Linux принято латать ядро, а старинные утилиты, которые перекочевывают из дистрибутива в дистрибутив, никто не анализирует и не переписывает. Например, последнее изменение в пакете kbd датируется 2002 годом [1].

Новые системы, создаваемые на базе Linux, просто копируют базовый дистрибутив и дополняют его, не проверяя содержимое этих дистрибутивов и не исследуя старые утилиты, содержащиеся в этих дистрибутивах, в итоге полу-